Responsible Artificial Intelligence Governance Policy

1. Purpose

USI ("the Company") is committed to the responsible, secure, transparent, and ethical development, acquisition, deployment, and use of artificial intelligence ("AI") across its operations, products, services, and supporting business processes.

This Policy establishes the Company's high-level governance expectations for AI so that innovation is supported by appropriate risk management, human accountability, information security, privacy protection, legal and ethical compliance, and continuous oversight. It is intended to promote trustworthy AI outcomes, reduce the likelihood of misuse or uncontrolled deployment, and provide a consistent basis for internal governance, audit review, and stakeholder assurance.

2. Scope

This Policy applies to all directors, officers, managers, employees, contractors, temporary personnel, and other authorized parties who use, manage, oversee, develop, procure, configure, integrate, or support AI on behalf of the Company. It applies to internally developed AI, externally procured AI services, general-purpose AI tools, agent-based AI capabilities, and AI-enabled features embedded in enterprise systems. The Policy covers the full AI lifecycle, including evaluation, design, acquisition, implementation, operation, monitoring, review, and retirement.

3. Governance and Oversight

The AI Governance Council shall provide centralized governance, oversight, and cross-functional coordination for the Company's AI activities. Its responsibilities include setting governance expectations, reviewing material AI risks, promoting consistent control implementation, and overseeing significant AI-related issues, including high-risk use cases, incidents, and exceptions.

The AI Governance Council shall be supported by relevant control and enabling functions, including Governance, Risk and Compliance, Security Architect, Privacy Legal, Intellectual Property Legal, Enterprise Architecture, and other business or technical stakeholders as appropriate. These functions shall contribute subject-matter expertise, challenge and review where needed, and support the implementation of governance requirements within their respective areas of responsibility.

Material AI risks, significant control deficiencies, major incidents, or high-impact use cases shall be escalated through the Company's governance structure to senior management, including the Information Security Steering Committee (ISSC), and, where appropriate, Board-level oversight, in accordance with the Company's established governance and reporting arrangements. This Policy shall be approved and endorsed at Board level through the Company's formal governance process for enterprise-level policies.

How it is implemented in USI

In USI, this is implemented through the establishment of the AI Governance Council in June 2026 as a cross-functional governance mechanism for AI oversight. The AI Governance Council reports to the Information Security Steering Committee (ISSC) and holds a regular monthly meeting to review the latest status of AI use across USI, track material governance developments, and review high-risk AI use cases that require additional oversight, challenge, or decision-making. Through the ISSC, the AI Governance Council is also able to provide regular reporting to Board-level oversight on the status of AI-related governance and management matters. Governance records of such meetings and related review outcomes shall be maintained in accordance with the Company's governance process.

4. Principles of Responsible AI

4.1 Reliability and Safety

AI systems shall be subject to an appropriate level of validation and testing before use or deployment, commensurate with their intended purpose and risk profile.

The Company shall maintain reasonable measures to monitor AI performance, reliability, and output quality over time, including the identification of abnormal behavior, degradation, misuse, or model drift, and shall take appropriate review, recalibration, retraining, or retirement actions where material performance concerns are identified.

Where material reliability or safety concerns are identified, the Company shall take timely corrective, restrictive, or discontinuation measures as appropriate.

How it is implemented in USI

In USI, this is implemented through a review process in which each introduced AI solution is reviewed by the AI Governance Council before or during adoption, as appropriate to the nature and risk of the use case. The cross-functional composition of the AI Governance Council is intended to ensure that such review covers the relevant areas of expertise required for reliability, safety, compliance, security, privacy, architecture, and legal considerations. USI also uses supporting tools, including Microsoft Purview, to strengthen compliance oversight for third-party AI services, and uses monitoring capabilities to support continuous monitoring of AI

use and the stability and reliability of AI-generated outputs over time. Records of relevant reviews, monitoring activities, and material findings shall be maintained in accordance with the Company's governance process.

4.2 Security

AI systems and related data shall be protected through appropriate information security controls, including access management, logging, monitoring, secure configuration, and encryption where applicable.

Security assessment and testing activities shall be applied according to the risk, criticality, and exposure of the AI system, including consideration of AI-specific threats where relevant. Such activities may include vulnerability assessment, penetration testing or equivalent security testing, and review of security configurations before production use and following material changes, as appropriate to the risk of the use case.

AI-related security events and weaknesses shall be addressed through the Company's established security incident management and resilience processes.

How it is implemented in USI

In USI, this is implemented through a combination of governance review, technical security controls, and continuous monitoring. For approved AI solutions, security requirements are considered as part of the review conducted by the AI Governance Council and relevant supporting functions, with particular attention to access control, secure configuration, data protection, and AI-specific security risks. USI applies identity and access management, least-privilege access, logging and monitoring, and other established information security controls to AI-related environments where applicable. For third-party or externally provided AI services, supporting tools and existing security governance mechanisms are used to strengthen oversight of security and compliance risks. In addition, security events, abnormal activities, or identified weaknesses related to AI use are handled through the Company's established security monitoring, incident management, and remediation processes. Records of relevant reviews, monitoring activities, and material security findings shall be maintained in accordance with the Company's governance process.

4.3 Privacy

AI use shall comply with the Company's data classification, data minimization, purpose limitation, retention, and secure handling requirements.

Use cases involving personal data, sensitive data, or elevated privacy impact shall be subject to appropriate privacy review and governance.

Privacy considerations shall be integrated across the AI lifecycle to support lawful, proportionate, and transparent processing of information.

How it is implemented in USI

In USI, this is implemented through data minimization checks, restrictions on the use of confidential or personal data in external AI environments, masking or de-identification where appropriate, lawful basis and purpose reviews for personal data processing, retention and deletion controls, and consultation with designated privacy or data protection functions for higher-risk use cases. USI also maintains Group-level Data Protection Officer (DPO) oversight and a set of privacy protection mechanisms designed to support compliance with applicable privacy requirements in the European Union, Asia, and North America, including privacy review and assessment processes such as DPIA where relevant. In addition, annual privacy protection training is provided to help employees understand personal data and how to protect it in the course of business activities, including where AI is used.

4.4 Fairness

Where relevant to the use case, especially for higher-risk AI, the Company shall consider whether bias, unfair treatment, or materially disparate outcomes may arise.

Reasonable monitoring, review, challenge, or fairness audit mechanisms shall be maintained to semi-annually to identify indications of bias, unfair treatment, or inappropriate outputs. For higher-risk use cases, such review shall be performed before deployment, following material changes, and periodically thereafter in accordance with the applicable governance process.

Where material fairness concerns are identified, remediation or additional control measures shall be considered as appropriate to the context and risk.

How it is implemented in USI

In USI, this is implemented through cross-functional review of introduced AI solutions by the AI Governance Council, with particular attention to the intended use, affected stakeholders, decision context, and whether the use case may create bias, unfair treatment, or materially disparate outcomes. The composition of the AI Governance Council helps ensure that relevant perspectives, including governance, privacy, legal, security, architecture, and business considerations, are reflected in the review. For higher-risk or sensitive use cases, additional review, challenge, or human oversight may be required before use or continued use is permitted. Where fairness concerns, bias indicators, or material review findings are identified, USI may require additional safeguards, usage restrictions, remediation actions, or further assessment as appropriate. In addition, USI emphasizes through user training that users are required to actively check AI-generated outputs and remain responsible for the content they use, rely on, or communicate. Records of relevant reviews, fairness assessments, training emphasis, and material decisions shall be maintained in accordance with the Company’s governance process.

4.5 Human Oversight

Human oversight shall be maintained at a level appropriate to the significance and risk of the use case, particularly where AI may materially influence decisions, actions, or external outcomes. Human oversight shall be ensured through appropriate control models, including human-in-command (final authority), human-on-the-loop (monitoring), or human-in-the-loop (approval required), depending on the risk level and use case.

Records of required human reviews, oversight actions, approvals, interventions, overrides, exceptions, and material decisions shall be documented and retained in accordance with the Company's governance and record-retention requirements. Such records shall provide evidence of meaningful human involvement and support accountability, traceability, auditability, and compliance with applicable legal, regulatory, and governance obligations.

AI shall not be treated as the sole decision-maker in sensitive, high-impact, or otherwise restricted matters unless expressly authorized under applicable governance and legal requirements.

How it is implemented in USI

In USI, this is implemented through governance arrangements that require meaningful human involvement in the review, approval, and use of AI, especially for higher-risk or materially consequential use cases. The AI Governance Council and relevant business or process owners help ensure that AI is not treated as an autonomous decision-maker in sensitive matters, and that appropriate human judgment remains part of the decision-making process. In practice, this includes approval checkpoints for higher-risk use cases, review of AI-generated outputs before they are used for consequential business actions or external communication, and clearly defined authority for designated personnel to challenge, override, restrict, suspend, or stop AI-supported activities where necessary. USI also emphasizes through training and governance requirements that users must actively review AI outputs, apply professional judgment, and remain accountable for the decisions or content they rely on, communicate, or implement. Records of required human review, oversight actions, exceptions, and material decisions shall be maintained in accordance with the Company's governance process.

4.6 Transparency

The Company shall promote transparency regarding the role of AI in relevant business processes, services, or outputs where such transparency is appropriate to context, law, contractual obligations, or stakeholder expectations.

For relevant use cases, the Company shall seek to ensure that appropriate users or reviewers can understand, to a level sufficient for responsible use, review, and effective human oversight, including:

- ✓ the intended purpose of the AI system;

- ✓ its key capabilities and limitations;
- ✓ the data sources or types of data used, where appropriate and permissible;
- ✓ the associated risks and uncertainties; and
- ✓ where reasonably practicable, the basis or rationale of AI-supported outputs.

AI-generated or materially AI-assisted content shall be labeled, disclosed, or otherwise identified where required by law, contract, governance requirements, or where omission could reasonably create misunderstanding regarding whether the content was generated by AI or by a human author or reviewer.

How it is implemented in USI

In USI, this is implemented through governance and communication practices that make the role of AI visible, understandable, and appropriately disclosed in relevant business activities. For introduced AI solutions, the intended use, the role of AI in the process, key limitations, and material assumptions are reviewed and documented as part of the governance process so that relevant users and reviewers understand how AI is being used and what constraints apply. Where AI-generated or materially AI-assisted content is used in business communication, deliverables, or other relevant scenarios, USI requires appropriate labeling, disclosure, or explanation when omission could create misunderstanding regarding the source, nature, or level of human involvement in the output. USI also emphasizes through training and governance requirements that users must understand the limitations of AI-generated content, verify outputs before use, and avoid presenting AI-supported results in a misleading or non-transparent manner. Records of relevant disclosures, governance reviews, and material decisions shall be maintained in accordance with the Company's governance process.

4.7 Accountability

Clear accountability for AI-related governance, operation, review, escalation, and remediation shall be assigned through the Company's governance structure and role responsibilities. Such accountability shall address, as applicable, errors, operational harm, compliance breaches, privacy impacts, security incidents, and legal or contractual consequences arising from AI use.

Material incidents, control failures, or governance concerns involving AI shall be investigated through appropriate management processes.

Corrective actions and improvement measures arising from AI-related reviews, assessments, incidents, or audits shall be tracked to closure as appropriate.

How it is implemented in USI

In USI, this is implemented through documented ownership of each approved AI use case, maintenance of approval and review records, recording of exceptions and risk acceptances, periodic management reporting on material issues, and retention of evidence sufficient to support internal review, external assurance, or audit where applicable. The AI Governance

Council oversees governance consistency and significant exceptions; business or process owners are accountable for the use of approved AI within their areas; and supporting functions such as Information Security, Privacy, Legal, IT, and GRC are responsible for review, investigation, or control actions within their respective mandates. In addition, relevant AI systems are required to maintain logs capable of recording key operations and outputs or results, so that material activities can be traced, reviewed, and investigated where necessary in accordance with the Company's governance and security processes.

4.8 Environmental Responsibility

Where relevant and reasonably practicable, the Company shall consider resource efficiency, proportionality, and broader environmental impact in the design, selection, and operation of AI capabilities. For AI systems hosted in Company-owned or externally provided data centers, the Company must also consider energy efficiency, carbon footprint, and sustainable infrastructure practices, including optimization of computing resources, cooling efficiency, and, where feasible, the use of renewable energy sources.

How it is implemented in USI

In USI, this is implemented through consideration of energy consumption, resource efficiency, and, where relevant, broader environmental factors in the selection or operation of material AI capabilities. For internally hosted AI systems, USI incorporates environmental considerations into data center operations, including monitoring of energy usage, optimization of compute workloads, and alignment with corporate sustainability objectives where applicable.

Where third-party or externally provided AI is used (e.g., Microsoft Copilot services), USI incorporates environmental and sustainability-related considerations into supplier selection and due diligence. This includes evaluating publicly available sustainability practices and disclosures from providers, such as Microsoft's published approach to improving data center energy efficiency, increasing the use of renewable energy, and optimizing AI workload efficiency.

Microsoft's sustainability initiatives include ongoing investments in energy-efficient data center operations, use of carbon-free electricity, and innovations in optimizing AI energy consumption and infrastructure efficiency, which support USI's evaluation of environmentally responsible AI providers. [https://learn.microsoft.com/en-us/industry/sustainability/advance-sustainability-ai]

In addition, the Company considers provider controls relating to security, confidentiality, transparency, licensing, and restrictions on secondary use of Company data as part of supplier governance and review, ensuring alignment with USI's sustainability, risk management, and responsible AI objectives.

5. Responsible Use

Only AI systems, models, tools, services, or enabled features that are approved, authorized, or otherwise permitted by the Company may be used for Company business.

Our company does not develop or deploy AI systems that fall under prohibited categories as defined by the EU AI Act, including manipulative systems, exploitation of vulnerable groups, social scoring, or unauthorized biometric surveillance.

AI shall be used only for legitimate business purposes and within the scope of the user's assigned responsibilities and authorized access.

Users remain responsible for exercising professional judgment and shall validate AI-generated outputs to an extent appropriate to the context before relying on them for business execution, internal decision-making, or external communication.

In addition, AI systems are subject to defined usage boundaries, including authorized scope, intended purpose, and capability limitations, to ensure they are used only within approved contexts and do not extend beyond their intended applications.

How it is implemented in USI

In USI, this is implemented through the use of an approved AI list and governance arrangements that require employees to use only authorized AI solutions for legitimate business purposes within defined use scenarios and assigned responsibilities.

Introduced AI solutions are reviewed through the Company's AI governance process before or during adoption, where the intended purpose, authorized scope, and key limitations of each use case are defined and documented to establish clear usage boundaries.

Approved use scenarios ensure that users understand what types of business activities are permitted and that AI systems are not applied beyond their intended context.

These boundaries are further reinforced through governance requirements and user training, which emphasize that users must follow applicable input and output handling rules, avoid the use of unapproved plug-ins or external AI tools, and not extend AI usage beyond approved purposes (i.e., preventing unintended use or mission creep).

In addition, control measures such as approval mechanisms, monitoring, and logging are applied to ensure that AI use remains within its defined boundaries. Users are required to actively validate AI-generated outputs before relying on them and remain accountable for the content, decisions, or communications they produce with AI support.

Records of approvals, defined usage boundaries, permitted use conditions, and material exceptions shall be maintained in accordance with the Company's governance process.

6. Prohibited Uses

Use of AI in a manner that results in unauthorized disclosure, transfer, retention, or exposure of Company, customer, employee, or other protected information is prohibited.

Fully automated AI decision-making in sensitive, restricted, or high-impact areas is prohibited unless specifically reviewed, approved, and governed under applicable requirements.

Unauthorized use of AI to execute cross-system actions, initiate transactions, perform mass processing, or bypass established controls, approvals, or segregation of duties is prohibited.

Illegal, deceptive, unethical, discriminatory, or otherwise prohibited uses of AI are not permitted, including uses inconsistent with applicable law, contractual obligations, or the Company's governance expectations. Prohibited practices include, where disallowed by applicable law or governance requirements, manipulative AI intended to materially distort behavior, unlawful social scoring, and unauthorized real-time biometric identification, surveillance, or similar monitoring activities.

How it is implemented in USI

In USI, this is implemented through a combination of governance restrictions, technical controls, and management escalation for non-permitted AI use. Non-approved external AI services, plug-ins, or integrations are restricted through existing access control, tenant, or network management measures where applicable, and suspected violations or high-risk exceptions are subject to management review and escalation through the Company's governance process.

For sensitive or high-impact AI use cases, USI applies enhanced access restrictions, including role-based access control (RBAC), least privileged principles, and, where applicable, prior approval or multi-level authorization before use. Such use cases may also be subject to additional monitoring, logging, and periodic review.

USI also emphasizes through governance requirements and user training that employees shall not bypass approved controls, use AI outside authorized business purposes, or use AI in a manner that could create material security, compliance, privacy, or ethical risks. Records of material violations, exceptions, and related management actions shall be maintained in accordance with the Company's governance process.

7. Risk Management

The Company shall apply a risk-based approach to AI governance, taking into account the intended purpose of the use case, the nature of the data involved, the degree of autonomy, the scale of impact, and the potential effect on individuals, operations, or compliance obligations.

AI use cases shall be subject to reassessment where material changes occur, including changes in purpose, data usage, integration scope, user population, decision impact, or external legal and regulatory conditions.

Higher-risk AI use cases shall be subject to enhanced review, governance attention, and control expectations, including stronger oversight and escalation where appropriate.

Approved AI use cases shall be subject to periodic monitoring or review to confirm that risk assumptions, governance conditions, and control effectiveness remain appropriate over time.

How it is implemented in USI

In USI, this is implemented through governance processes that require introduced AI solutions and use cases to be reviewed, classified, and tracked according to their nature, intended use, data sensitivity, degree of autonomy, and potential business or compliance impact. The AI Governance Council reviews material AI use cases, with higher-risk scenarios receiving enhanced review and additional governance attention before or during adoption, as appropriate. Where material changes occur, such as changes in purpose, data use, integration scope, or decision impact, the relevant use case is subject to reassessment through the Company's AI governance process. USI also maintains periodic review of approved AI use cases so that evolving risks, control effectiveness, and governance conditions can be evaluated over time. Records of use case reviews, risk classifications, reassessments, and material governance decisions shall be maintained in accordance with the Company's governance process.

8. Data Protection

Data used with AI shall be handled in accordance with the Company's information classification and protection requirements and shall be limited to what is necessary and authorized for the relevant purpose.

Sensitive, confidential, personal, or otherwise restricted data shall not be used with external or non-approved AI environments except as expressly permitted under applicable governance, security, privacy, and legal requirements.

AI-related data handling shall, where appropriate, be integrated with the Company's monitoring, logging, retention, and incident response capabilities to support accountability and auditability.

How it is implemented in USI

In USI, this is implemented through data governance measures that require information used with AI to follow the Company's data classification and protection requirements, including restrictions on the use of confidential, personal, or otherwise restricted data in non-approved or

external AI environments. Where enterprise data sources are connected to AI services, appropriate approval and governance review are required in advance, and relevant data access, transfer, or use activities are subject to logging and monitoring where applicable. USI also applies retention, deletion, and access control measures as part of its broader information security and data protection framework, and uses supplier or contractual controls to address confidentiality, security, and restrictions on secondary use of Company data by third-party AI providers. Records of relevant approvals, monitoring activities, and material data protection findings shall be maintained in accordance with the Company's governance process.

9. Training and Awareness

The Company shall maintain training and awareness activities to support responsible, secure, and compliant use of AI. Such training shall be provided to relevant users upon onboarding or prior to access where appropriate, refreshed periodically thereafter, and updated following material changes in governance requirements, technology, or risk conditions.

Training content may include AI governance principles, information security, privacy protection, output validation, appropriate use restrictions, and awareness of shadow AI and misuse risks.

Training and awareness measures may be tailored according to roles, responsibilities, and the nature of AI use within the Company.

How it is implemented in USI

In USI, this is implemented through AI-related training provided during employee onboarding and on an annual basis, together with role-based training for relevant users, guidance on acceptable prompts and data handling, awareness of common AI failure modes, and targeted reinforcement for teams using higher-risk or business-critical AI capabilities. USI also regularly distributes additional AI-related training and awareness content to employees through newsletters and similar communication channels to reinforce key governance, security, privacy, and responsible use expectations. Training audiences may include general users, developers, administrators, approvers, reviewers, or other roles with elevated AI-related responsibilities.

10. Reporting Mechanism

Concerns relating to AI, including suspected misuse, control weaknesses, material errors, security events, privacy concerns, ethical issues, or complaints about materially consequential AI-supported outcomes, may be reported through the Company's established reporting, ethics, security, privacy, or compliance channels. Where an applicable process provides for complaint or appeal intake, the Company shall provide a reasonably accessible channel and shall review and respond in accordance with the relevant governance process.

Reported matters shall be reviewed and addressed through the Company's established governance and investigation processes, with corrective or preventive actions taken as appropriate.

How it is implemented in USI

In USI, this is implemented through existing reporting and escalation channels for security, privacy, compliance, ethics, or other governance concerns, which may also be used to report AI-related issues. The company shall also provide an AI-specific external reporting channel, when AI services are provided to external clients and third parties. Reported concerns, including suspected misuse, abnormal outputs, control weaknesses, or material incidents, are reviewed and routed according to their nature and severity, with relevant functions involved as appropriate. Where needed, material AI-related concerns may be escalated through the Company's governance process, including review by the AI Governance Council. USI also maintains records of material reports, investigations, follow-up actions, and remediation outcomes in accordance with the Company's governance process.

11. Governance Metrics

The Company may monitor governance metrics to support oversight and continuous improvement of its AI governance program.

Examples may include the number and type of approved AI systems or use cases, reported incidents or concerns, and the status of remediation activities.

The Company may also track training coverage, governance review activities, policy exceptions, environmental or resource-efficiency indicators relevant to material AI use, or other indicators relevant to risk visibility and program maturity.

Relevant audit observations, review outcomes, or recurring issues may be used to inform improvement priorities and management reporting.

How it is implemented in USI

In USI, this is implemented through periodic governance reporting and metric review that support ongoing oversight of AI-related management matters. Outputs from the monthly review activities of the AI Governance Council may be used to inform governance metrics, trend analysis, follow-up actions, and management reporting. Such metrics may include the status of approved AI use cases, high-risk case reviews, reported incidents or concerns, training completion, remediation progress, and other indicators relevant to the effectiveness and maturity of AI governance. Through the Information Security Steering Committee (ISSC), relevant governance reporting may also support regular visibility of AI-related management

status at Board level. Records of relevant metrics, reports, and material follow-up actions shall be maintained in accordance with the Company's governance process.

12. Policy Management

This Policy shall be reviewed periodically and updated as appropriate to reflect changes in business use, technology, risk conditions, and applicable legal or regulatory expectations.

The AI Governance Council is responsible for maintaining this Policy and overseeing its implementation through the Company's governance framework.

13. Violations and Exceptions

Violations of this Policy may result in disciplinary or other management action in accordance with applicable Company rules, contractual arrangements, and local legal requirements.

Any exception to this Policy shall be subject to an appropriate approval and risk acceptance process consistent with the Company's established governance requirements.

Appendix

The Appendix provides an illustrative summary of prohibited and high-risk AI practices, including manipulation, unlawful surveillance, discriminatory use, unauthorized autonomous actions, and AI use cases in sensitive domains such as employment, finance, production control, and other scenarios that may require enhanced governance review.

Table 1: List of Illegal (Prohibited) AI Practices

The following AI practices violate applicable laws and regulations or seriously breach fundamental ethical principles. They constitute governance red lines of the Company and are strictly prohibited from development, procurement, or use under any circumstances.

Category	**Governance Red Line (Principle-Based)**	**Representative Examples (Non-Exhaustive)**
Manipulation and Deception	Using AI to manipulate individuals' decisions, behavior, or cognition without their awareness or against their genuine intent	• Subliminal or psychological manipulation influencing individual choices • Use of deepfake content to impersonate others or mislead the public

Exploitation of Vulnerable Groups	Targeting vulnerable populations (e.g., children, elderly, persons with disabilities, economically disadvantaged) by exploiting their particular vulnerabilities	• AI-driven inducement of elderly individuals into unnecessary purchases or financial decisions • Collection or misuse of personal data of minors
Unlawful Surveillance and Privacy Infringement	Deploying AI for large-scale surveillance, tracking, or biometric identification without legal authorization or explicit consent	• Unauthorized facial recognition or biometric monitoring • AI-based inference of employee emotions, psychological states, or behavioral tendencies
Social Scoring and Discrimination	Using AI to classify, score, or treat individuals or groups in a socially discriminatory manner	• Social credit scoring impacting access to services or opportunities • Discriminatory treatment based on protected characteristics such as race, gender, or age
Public Safety and Illegal Use	Applying AI for unlawful activities or purposes that endanger public or national security	• Assisting cyberattacks, data theft, or fraud • Generating falsified evidence or forged legal or commercial documents

Table 2: List of High-Risk AI Practices

High-Risk Domain	**Risk Description (Principle-Based)**	**Representative Examples (Non-Exhaustive)**
Human Resources and Personnel Management	AI systems affecting employment opportunities, career development, or labor relations	• Recruitment screening, résumé evaluation, interview scoring • Performance assessment, promotion, compensation, or termination recommendations
Financial, Credit, and Major Transactions	AI systems producing significant economic impact on individuals or the organization	• Credit approval, insurance pricing, or claims decisions • Large fund transfers, investments, or asset disposals

Critical Infrastructure and Production Control	AI systems influencing safety, operational continuity, or system stability	• Production line control, equipment scheduling, or quality determination • Energy management, supply chain, or logistics control
Automated Decision-Making with Legal Effect	Automated decisions producing legal or similarly significant effects	• Fully automated service denial, penalties, or restrictions • Contract generation, legal or compliance determinations
Agentic AI (Autonomous / Agent-Based AI)	AI systems with autonomous decision-making and cross-system execution capabilities	• AI agents executing tasks across enterprise systems using employee credentials • AI systems autonomously planning and executing business workflows
Sensitive Social Domains	AI systems applied in highly regulated or public-interest areas	• Educational assessment, exam scoring, or academic placement • Medical diagnosis, treatment recommendations, or health risk assessment